IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Art Unit: 2435

J. Scott Carr Conf. No.: 3480

Application No.: 10/686,547

Filed: October 14, 2003 **Via Electronic Filing**

For: Digital Watermarking for Identification Documents

Examiner: Leynna T. Truvan

Date: September 28, 2010

APPEAL BRIEF

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellants respectfully request the Board of Patent Appeals and Interferences (hereafter the "Board") to reverse the outstanding final rejection of the pending claims.

This Appeal Brief is in furtherance of a Notice of Appeal filed May 24, 2010, and is responsive to the final Office Action mailed January 22, 2010 ("final Office Action").

Please charge the fee required under 37 CFR 1.17(f) and any other fees needed to consider this Appeal Brief to our deposit account no. 50-1071.

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party in interest is Digimarc Corporation headquartered in Beaverton, Oregon.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

Claims 1-12, 14-25 and 27-57 are pending in the present application.

Claims 1-12 and 14-20, 25, 27-29 and 52-57 stand finally rejected and are on appeal.

Claims 21-24 and 30-51 are withdrawn from consideration.

Claims 13 and 26 were previously canceled.

STATUS OF AMENDMENTS

All earlier-filed amendments have been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

Claim 1 recites a method of verifying an age of a bearer of a document [see original claim 1; see also page 14, paragraph [0053] – page 16, paragraph [0057]]. The method comprises: receiving first digital data corresponding to an age indicator, the first digital data being obtained from auxiliary data steganographically embedded in the document [see, e.g., page 16, paragraphs [0055] - [0057]]; receiving second digital data corresponding to a biometric indictor, the second digital data being obtained from auxiliary data steganographically embedded in the document; receiving third digital data corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer; and verifying the bearer's age when: i) the first digital data indicates that the bearer is at least as old as a predetermined age, and ii) the second digital data and the third digital data correspond [see, e.g., page 16, paragraphs [0055] - [0057]].

Claim 12 recites a method of anonymously verifying an age or characteristic associated with a person, the person being in possession of an identification document, the identification document including a document layer and printing carried by the document layer, the identification document further including a digital watermark embedded therein, the digital watermark including a first set of information, the first set of information including information to verify age or an age level of the person [see, e.g., page 40, original claim 12]. The method comprises: receiving optical scan data corresponding to the identification document, the optical scan data being generated by an optical sensor; decoding the scan data with a configured multi-purpose electronic processor to obtain the first set of information included in the digital watermark [see, e.g., page 15, paragraph [0054]], the first set of information including a concatenated string of data comprising an age indicator and additional data [see, e.g., page 18, paragraphs [0061]-[0062]], wherein the digital watermark is embedded in the identification document through hidden changes to data representing one or more items carried by the identification document [see, e.g., pages 2-3, paragraph [0007] and page 18, paragraphs [0061]-[0062]]; and determining, based on the first set of information, the person's age or age level in connection with an age-related transaction or event, wherein said act of determining protects the anonymity of the person in possession of the identification document from said multi-purpose electronic processor or entity performing said determining [see, e.g., pages 17 and 18, paragraphs [0061]-[0063]].

Claim 14 recites the method of claim 12, wherein the identification document further comprises a second set of information embedded therein, the second set of information corresponding to a third set of information that is printed on the identification document, wherein the second set of information comprises an index for accessing a data repository [see, e.g., pages 11 and 12, paragraph [0044] and pages 31-32, paragraph [0102]].

Claim 15 recites the method of claim 14, wherein the index comprises a hash of the third set of information that is printed on the identification document [see, e.g., paragraph [0060]].

Claim 18 recites the method of claim 17, wherein the first set of information comprises two or more random bits [see, e.g., pages 17 and 18, paragraphs [0061]-[0063]].

Claim 20 recites the method of claim 19, wherein a combination of the random bits and the date of birth decrease likelihood of overlapping birth dates, while maintaining an anonymous audit clue [see, e.g., pages 17 and 18, paragraphs [0061]-[0063]].

Claim 25 recites a method comprising: receiving optical scan data that is associated with an identification document, the identification document comprising plural-bits of data carried by the identification document [see, e.g., page 15, paragraph [0054]], wherein the plural-bits of data comprise at least a first field and a second field, the first field carrying or linking to information corresponding to a bearer of the identification document [see, e.g., pages 14 and 15, paragraph 53, and see page 16, paragraph [0055]] and the second field corresponding to an age or age level of the bearer of the identification document [see, e.g., page 16, paragraph [0055]] ; utilizing a configured multi-purpose electronic processor, decoding the optical scan data to recover data corresponding to at least the second field [see, e.g., page 15, paragraph [0054]; see also page 16, paragraph [0055]]; receiving information carried by the document – separate from the data corresponding to at least the second field – and generating a reduced-bit representation of the received information by using a configured multi-purpose electronic processor [see, e.g., pages 15 and 16, paragraph [0054]; and comparing data corresponding to the second field with the reduced-bit representation to verify an age level associated with the document in connection with an age-related transaction or event [see, e.g., page 15, paragraph [0054] – page 17, paragraph [0059]], wherein neither the data corresponding to the second field nor the reduced-bit representation betray the identity of the bearer of the identification document to said multi-purpose electronic processor or an entity performing said act of comparing [see, e.g., page 17, paragraphs [0059]-[0060]].

Claim 27 recites the method of claim 25 further comprising storing the data corresponding to the second field in a data repository to evidence examination of the identification document [see, e.g., page 17, paragraph [0060]].

The above specification citations should not be construed as limiting claim scope. Of course, additional and alternative support can be found throughout the application as well.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-12, 14-20, 25, 27-29 and 52-57 stand finally rejected under 35. U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,748,533 (hereafter referred to as "the Wu patent" or simply as "Wu") in view of US Patent No. 7,159,116 (hereafter referred to as "the Moskowitz patent" or simply as "Moskowitz").

ARGUMENT

Rejections under 35 U.S.C. § 103(a) over the Wu patent and the Moskowitz patent

Claim 25 (and dependent claims 28, 29, 56 and 57)

Independent claim 25 recites:

25. A method comprising:

receiving optical scan data that is associated with an identification document, the identification document comprising plural-bits of data carried by the identification document, wherein the plural-bits of data comprise at least a first field and a second field, the first field carrying or linking to information corresponding to a bearer of the identification document and the second field corresponding to an age or age level of the bearer of the identification document;

utilizing a configured multi-purpose electronic processor, decoding the optical scan data to recover data corresponding to at least the second field;

receiving information carried by the document – separate from the data corresponding to at least the second field – and generating a reduced-bit representation of the received information by using a configured multi-purpose electronic processor; and

comparing data corresponding to the second field with the reduced-bit representation to verify an age level associated with the document in connection with an age-related transaction or event,

wherein neither the data corresponding to the second field nor the reduced-bit representation betray the identity of the bearer of the identification document to said multi-purpose electronic processor or an entity performing said act of comparing.

Claim 25 recites – in combination with other features – comparing data corresponding to the second field with the reduced-bit representation to verify an age level associated with the document *in connection with an age-related transaction or event.* Neither the data corresponding to the second field nor the reduced-bit representation betray the identity of the bearer of the identification *document to said multi-purpose electronic processor or an entity performing said act of comparing.*

The final Office Action stated that Wu protects a person's anonymity by encrypting data to protect the owner from unauthorized people. See the final Office Action, page 8, 2nd to last line – page 9, line 3.

Surely, however, the *intended* receiving party would need to decrypt the data for Wu's verification purposes, which could betray the identity of the document bearer. Thus, Wu lacks the claim feature of not betraying the identity of the bearer of the identification *document to the multi-purpose electronic processor or an entity performing said act of comparing*, as recited in claim 25.

It is also worth noting the final Office Action's discussion on page 5, lines 15-17, which alleges that Moskowitz discloses protecting a person's anonymity. Moskowitz is cited at Col. 20, line 60 and Col. 38, lines 3-8, for these features. Moskowitz at Col. 38, lines 3-8, discusses "anonymous authentication" for a product, medicine or label. In response, an authentication device may display known warnings or recommended dosages regarding the "**item**" in question. Thus, there is no discussion there of verifying an age level associated with a document *in connection with an age-related transaction or event.* When dealing with verifying the identity of an individual, Moskowitz requires additional "identity" verification. See Moskowitz at Col. 38, lines 16-22. We also do not see any mention of an age-related transaction or event at Moskowitz Col. 20, line 60.

Regarding Wu, the final Office Action admits that Wu includes "personal particulars" in its identification. See the final Office Action, page 4, lines 6-7 of paragraph titled "Regarding argument for claim 25…."

Thus, even if combined as proposed in the final Office Action, Wu and Moskowitz would not render obvious claim 25's features – in combination with other features – of comparing data corresponding to the second field with the reduced-bit representation to verify an age level associated with the document *in connection with an age-related transaction or event*. Neither the data corresponding to the second field nor the reduced-bit representation *betray the identity of the bearer of the identification document to said multi-purpose electronic processor or an entity performing said act of comparing*.

We respectfully request the Board to reverse the final rejection of claim 25.

Claim 27

Dependent claim 27 recites:

27. The method of claim 25 further comprising storing the data corresponding to the second field in a data repository to evidence examination of the identification document.

Claim 27 recites *storing the data* corresponding to the second field in a data repository *to evidence examination of the identification document*.

Wu is cited at Col 7, lines 35-37 and Col. 4, lines 48-55 for these features. See the final Office Action, page 19, lines 4-6.

We respectfully submit that one of ordinary skill in the art will disagree.

For example, Col 4 discusses verifying the legitimacy of an article against forgery. And the Col. 7 passage discusses what kind of articles can be protected against forgery (e.g., a credit card, driver's license, etc.).

Neither of the cited passages, however, discusses *storing data to evidence examination of the identification document*.

The final Office Action further states that: "By verifying is to evidence examination of the identification document and thus by containing the watermark/cryptographic data must be stored in order to verify the legitimacy of the document (col. 2, lines 43-47)." See the final Office Action, page 2, lines 8-11 of paragraph 3. We respectfully submit that this misstates the cited Wu passage, and mis-interrupts the claim language. The cited passage passage is reproduced below for convenience.

> *In accordance with a third aspect of the invention, there is disclosed a computer program product having a computer readable medium having a computer program recorded therein for embedding linked watermarks in an article requiring protection against forgery....*

While this passage discusses a computer program for embedding watermarks, we see no discussion there of storing data to evidence examination of an identification document as recited in claim 27.

We respectfully request the Board to reverse the final rejection of claim 27.

Claim 12 (and dependent claims 17, 54 and 55)

Independent claim 12 recites:

12. A method of anonymously verifying an age or characteristic associated with a person, the person being in possession of an identification document, the identification document including a document layer and printing carried by the document layer, the identification document further including a digital watermark embedded therein, the digital watermark including a first set of information, the first set of information including information to verify age or an age level of the person, said method comprising:

receiving optical scan data corresponding to the identification document, the optical scan data being generated by an optical sensor;

decoding the scan data with a configured multi-purpose electronic processor to obtain the first set of information included in the digital watermark, the first set of information including a concatenated string of data comprising an age indicator and additional data,

wherein the digital watermark is embedded in the identification document through hidden changes to data representing one or more items carried by the identification document; and

determining, based on the first set of information, the person's age or age level in connection with an age-related transaction or event, wherein said act of determining protects the anonymity of the person in possession of the identification document from said multi-purpose electronic processor or entity performing said determining.

Claim 12 recites – in combination with other features – determining, based on the first set of information, the person's age or age level *in connection with an age-related transaction or event*, wherein said act of *determining protects the anonymity of the person in possession of the identification document from said multi-purpose electronic processor or entity performing said determining*.

The Wu document is cited at col. 7, lines 20-28 and line 65-Col. 8, lines 3 as meeting portions of the act of determining. See the final Office Action at page 12, 3rd full paragraph. These passages include "information related to the product owner's identity." See Col. 7, line 20. But, surely, information related to the owner's identity does not *protect the anonymity of the person in possession of the identification document* as recited in claim 12.

The final Office Action further stated that Wu protects a person's anonymity by encrypting data to protect the owner from unauthorized people. See the final Office Action, page 13, line 19 – page 14, line 2. Surely, however, the *intended* receiving party would need to decrypt the data, e.g., for verification, which could betray the identity of the document bearer. Thus, Wu lacks the claim feature of protecting the anonymity of the person in possession of the identification document from the multi-purpose electronic processor or entity performing the determining.

It is also worth noting the final Office Action's discussion on page 14, lines 4-5, which alleges that Moskowitz discloses protecting a person's anonymity. Moskowitz is cited at Col. 20, line 60 and Col. 38, lines 3-8, for these features. Moskowitz at Col. 38, lines 3-8, discuss "anonymous authentication" for a product, medicine or label. In response, an authentication

device may display known warnings or recommended dosages regarding the "**item**" in question. There is no discussion there of verifying an age level associated with a document *in connection with an age-related transaction or event*. When dealing with verifying the identity of an individual, Moskowitz requires additional "identity" verification. See Moskowitz at Col. 38, lines 16-22. We also do not see any mention of an age-related transaction or event at Moskowitz Col. 20, line 60.

Thus, even if combined as proposed in the final Office Action, Wu and Moskowitz would not render obvious claim 12' features – in combination with other features – of determining, based on the first set of information, the person's age or age level *in connection with an age-related transaction or event*, wherein said act of *determining protects the anonymity of the person in possession of the identification document from said multi-purpose electronic processor or entity performing said determining*.

We respectfully request the Board to reverse the final rejection of claim 12.

Claim 14 (and dependent claim 16)

Dependent claim 14 recites:

14. The method of claim 12, wherein the identification document further comprises a second set of information embedded therein, the second set of information corresponding to a third set of information that is printed on the identification document, wherein the second set of information comprises an index for accessing a data repository.

Claim 14 recites a second set of information embedded in the identification document of claim 12. The second set of information corresponds to a third set of information that is printed on the identification document. The second set of information comprises an ***index*** *for accessing a data repository*.

Regarding the features of claim 14, Wu at Col. 7, line 53 – Col. 8, line 3, is cited in the final Office Action (see page 15, lines 2-6).

The cited Wu passage, however, discusses storing different information (i.e., identification portion, name of country or state, photograph, passport number, name of person, issuance information, personal particulars and biometric data) and does not mention a second set of information comprising an ***index*** *for accessing a data repository.*

Wu is also cited at Col. 8, lines 43-47. See the final Office Action, page 2, last paragraph. We see mention of a cryptographic watermark link in the cited Wu passage, but no mention of a second set of information comprising an index for accessing a data repository.

Claim 14 should be allowed since Wu does not have or render obvious the features of claim 14, and Moskowitz is not cited to cure any of Wu's deficiencies. Thus, the rejection based on Wu and Moskowitz does not provide a *prima facie* case of obviousness.

We respectfully request the Board to reverse the final rejection of claim 14.

Claim 15

Dependent claim 15 recites:

15. The method of claim 14, wherein the index comprises a hash of the third set of information that is printed on the identification document.

Claim 15 recites that the *index comprises a hash* of the third set of information that is printed on the identification document. (Recall from claim 14 that the index is for accessing a data repository.)

The cited Wu passage (col. 8, lines 22-30; see the final Office Action, page 15, lines 7-9) discusses encrypting a biometric invariant feature with a hash. But this hash is not an index for accessing a data repository.

Wu does not have or render obvious the features of claim 15, and Moskowitz is not cited to cure any of Wu's deficiencies. Thus, the rejection based on Wu and Moskowitz does not provide a *prima facie* case of obviousness.

We respectfully request the Board to reverse the final rejection of claim 15.

Claim 18 (and dependent claim 19)

Dependent claim 18 recites:

18. The method of claim 17, wherein the first set of information comprises two or more random bits.

Claim 18 recites a first set of information comprising two or more random bits. The final Office Action perhaps refers to the "generate random pattern" step 608 of Wu's with its citation to Fig. 6. See the final Office Action, page 15, last 2 lines – page 16, line 1.

We respectfully submit that one of ordinary skill in the art will disagree.

Claim 18's "first set of information" is like a message, and if mapped to Wu's Fig. 6 would be more like the biometric information 600 or the other appending information 602. Information 600 and 602 are encrypted and provided to a random pattern generator. But, as a result, the biometric information 600 and the other appending information 602, themselves, do not then include "two or more random bits". We submit that the random pattern is more akin to a watermark carrier signal, and not to an actual message.

The final Office Action also cites Wu at Col. 11, lines 15-18 (see page 15, last two lines) and Wu at Col. 8, lines 28-30 (see page 3, line 5-8). We take these in turn.

First, the Col. 11, lines 15-18 passage discusses invariant biometric features 516 output to a watermark generator. Invariant features are discussed at Col. 11, lines 10-14. For example, these are features are computed by a projection of an input facial image onto eigenfaces. We do not see mention of two or more random bits as used in claim 18.

Second, the Col. 8, lines 28-30 passage discusses encryption, but it does not say that the first set of information, itself, includes two or more random bits. Please see our related discussion, above regarding Fig. 6.

Wu does not have or render obvious the features of claim 18, and Moskowitz is not cited to cure any of Wu's deficiencies. Thus, the rejection based on Wu and Moskowitz does not provide a *prima facie* case of obviousness.

We respectfully request the Board to reverse the final rejection of claim 18.

Claim 20

Dependent claim 20 recites:

20. The method of claim 19, wherein a combination of the random bits and the date of birth decrease likelihood of overlapping birth dates, while maintaining an anonymous audit clue.

Claim 20 recites – in combination with other features – that a combination of random bits and the date of birth decrease likelihood of overlapping birth dates, while maintaining an anonymous audit clue.

We see no mention of "maintaining an anonymous audit clue," in combination with the other claim features, in the cited passages (see the final Office Action, page 16, lines 4-7, citing Wu at col. 11, lines 15-18 and Fig. 6). Indeed, the cited Wu passage at col. 11, lines 15-18 (and fig. 6), says nothing regarding maintaining an anonymous audit clue, in combination with the other claim features.

On page 3, lines 9-13, the final Office Action states that Wu's (at Col. 8, lines 23-57) watermarking, encryption and hashing of data is the claimed "anonymous audit clue." We respectfully submit that one of ordinary skill in the art will disagree. For example, these passages discuss using people's photographs, biometrics and fingerprints. Such personal – and identifying – information does not provide an anonymous audit clue.

Wu does not have or render obvious the features of claim 20, and Moskowitz is not cited to cure any of Wu's deficiencies. Thus, the rejection based on Wu and Moskowitz does not provide a *prima facie* case of obviousness.

We respectfully request the Board to reverse the final rejection of claim 20.

Claim 1 (and dependent claims 2-11)

Independent claim 1 recites:

1. A method of verifying an age of a bearer of a document, said method comprising:

receiving first digital data corresponding to an age indicator, the first digital data being obtained from auxiliary data steganographically embedded in the document;

receiving second digital data corresponding to a biometric indictor, the second digital data being obtained from auxiliary data steganographically embedded in the document;

receiving third digital data corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer; and

verifying the bearer's age when: i) the first digital data indicates that the bearer is at least as old as a predetermined age, and ii) the second digital data and the third digital data correspond.

Claim 1 recites – in combination with other features – ***verifying a bearer's age when***: i) the first digital data indicates that the bearer is at least as old as a predetermined age, **and** ii) the second digital data and the third digital data correspond.

Both conditions i and ii must be satisfied in order to *verify a bearer's age*.

Wu at Col. 7, lines 20-28 (see final Office Action, page 7, 2nd to last paragraph) mentions the term "Birth date" (line 21) but says nothing of verifying a bearer's age when first digital data indicates that the bearer is at least as old as a predetermined age. And while Wu at Col. 5, lines 14-33 and Col. 9, lines 1-22 (see final Office Action, page 7, 2nd to last paragraph) may discuss verifying the legitimacy of an article, neither passage discusses *verify a bearer's age* when second digital data and the third digital data correspond.

Therefore, even if combined as suggested, Wu and Moskowitz would not provide a method or system to verify a bearer's age when: i) the first digital data indicates that the bearer is at least as old as a predetermined age, and ii) the second digital data and the third digital data correspond.

We respectfully request the Board to reverse the final rejection of claim 1.

CONCLUSION AND REQUEST FOR REVERSAL

Appellants respectfully request the Board to reverse the final rejections of the pending claims.

Respectfully submitted,

Date: September 28, 2010

DIGIMARC CORPORATION

Customer No. 23735

Telephone: 503-469-4685
FAX: 503-469-4777

By: /Steven W. Stewart, Reg. No. 45,133/
Steven W. Stewart
Registration No. 45,133

CLAIMS APPENDIX

1. (previously presented): A method of verifying an age of a bearer of a document, said method comprising:

receiving first digital data corresponding to an age indicator, the first digital data being obtained from auxiliary data steganographically embedded in the document;

receiving second digital data corresponding to a biometric indictor, the second digital data being obtained from auxiliary data steganographically embedded in the document;

receiving third digital data corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer; and

verifying the bearer's age when: i) the first digital data indicates that the bearer is at least as old as a predetermined age, and ii) the second digital data and the third digital data correspond.

2. (original): The method of claim 1, further comprising interrogating a data repository with the biometric indictor to obtain the second digital data.

3. (original): The method of claim 2, further comprising interrogating the data repository with the age indictor to obtain the first digital information.

4. (original): The method of claim 2, wherein the second digital data comprises a biometric template associated with the bearer.

5. (previously presented): The method of claim 4, wherein the biometric template includes information associated with at least one of the bearer's fingerprint, face map, hand geometry, iris, retina, DNA, voiceprint or vein pattern.

6. (original): The method of claim 1, wherein the third digital data is received through a network.

7. (original): The method of claim 6, wherein the network comprises the internet.

8. (original): The method of claim 1, wherein the biometric indicator comprises a biometric template.

9. (previously presented): The method of claim 8, wherein the biometric template includes information associated with at least one of the bearer's fingerprint, face map, hand geometry, iris, retina, DNA, voiceprint or vein pattern.

10. (original): The method of claim 1, wherein the third digital data further comprises a timestamp.

11. (original): The method of claim 4, wherein the auxiliary data comprises plural bits of data and wherein the biometric indicator and the age indicator comprise the same plural bits.

12. (previously presented): A method of anonymously verifying an age or characteristic associated with a person, the person being in possession of an identification document, the identification document including a document layer and printing carried by the document layer, the identification document further including a digital watermark embedded therein, the digital watermark including a first set of information, the first set of information including information to verify age or an age level of the person, said method comprising:

receiving optical scan data corresponding to the identification document, the optical scan data being generated by an optical sensor;

decoding the scan data with a configured multi-purpose electronic processor to obtain the first set of information included in the digital watermark, the first set of information including a concatenated string of data comprising an age indicator and additional data, wherein the digital

watermark is embedded in the identification document through hidden changes to data representing one or more items carried by the identification document; and

determining, based on the first set of information, the person's age or age level in connection with an age-related transaction or event, wherein said act of determining protects the anonymity of the person in possession of the identification document from said multi-purpose electronic processor or entity performing said determining.

13. canceled.

14. (original): The method of claim 12, wherein the identification document further comprises a second set of information embedded therein, the second set of information corresponding to a third set of information that is printed on the identification document, wherein the second set of information comprises an index for accessing a data repository.

15. (original): The method of claim 14, wherein the index comprises a hash of the third set of information that is printed on the identification document.

16. (previously presented): The method of claim 14, further comprising computing a hash of the third set of information that is printed on the identification document, decoding the second set of information that is embedded in the identification document to obtain the embedded hash, and comparing the computed hash and the embedded hash to determine authenticity of the document.

17. (previously presented): The method of claim 12, further comprising storing at least a portion of the first set of information in at least one of a list, electronic memory circuits or a data record, wherein the stored portion of the first set of information serves as an audit clue to evidence that the identification document has been examined.

18. (original): The method of claim 17, wherein the first set of information comprises two or more random bits.

19. (original): The method of claim 18, wherein the first set of information comprises a date of birth.

20. (original): The method of claim 19, wherein a combination of the random bits and the date of birth decrease likelihood of overlapping birth dates, while maintaining an anonymous audit clue.

21. (withdrawn): A security document comprising:

a substrate; and

a first printed area carried by the substrate, the first printed area being steganographically encoded to secretly convey first plural bits of digital data recoverable by computer analysis of said first printed area, wherein the first printed area comprising an ink that is designed to degrade or rub off with use, thereby removing the steganographic encoding from the security document.

22. (withdrawn): The method of claim 21, wherein the steganographic encoding comprises a digital watermark.

23. (withdrawn): A security document comprising:

a substrate;

a first printed area carried by the substrate, the first printed area being steganographically encoded to secretly convey first plural bits of digital data recoverable by computer analysis of said first printed area; and

a second ink applied over the first ink in the first printed area, the second ink having a relatively lower adhesion property in comparison to the first ink, wherein the first plural bits of digital data are recoverable by computer analysis of the first printed area only after the second ink

degrades or is removed from the security document.

24. (withdrawn): The method of claim 23, wherein the steganographic encoding comprises a digital watermark.

25. (previously presented): A method comprising:

receiving optical scan data that is associated with an identification document, the identification document comprising plural-bits of data carried by the identification document, wherein the plural-bits of data comprise at least a first field and a second field, the first field carrying or linking to information corresponding to a bearer of the identification document and the second field corresponding to an age or age level of the bearer of the identification document;

utilizing a configured multi-purpose electronic processor, decoding the optical scan data to recover data corresponding to at least the second field;

receiving information carried by the document – separate from the data corresponding to at least the second field – and generating a reduced-bit representation of the received information by using a configured multi-purpose electronic processor; and

comparing data corresponding to the second field with the reduced-bit representation to verify an age level associated with the document in connection with an age-related transaction or event,

wherein neither the data corresponding to the second field nor the reduced-bit representation betray the identity of the bearer of the identification document to said multi-purpose electronic processor or an entity performing said act of comparing.

26. canceled.

27. (previously presented): The method of claim 25 further comprising storing the data corresponding to the second field in a data repository to evidence examination of the identification document.

28. (previously presented): The method of claim 25 further comprising printing the data corresponding to the second field to evidence examination of the identification document.

29. (previously presented): The method of claim 25, wherein said receiving information carried by the document comprises receiving data corresponding to at least one of data generated by a barcode scanner, optical character recognizer, manual entry or watermark decoder.

30. (withdrawn): A method of embedding watermark information in an image captured by a digital camera, comprising:

capturing an image of a human subject;

identifying a face region in the captured image of the human subject;

realigning the captured image of the human subject within an image frame based at least in part on the identified face region; and

embedding the watermark information in the realigned captured image.

31. (withdrawn): The method of claim 30 wherein realigning the captured image comprises centering the image within predetermined image frame dimensions.

32. (withdrawn): The method of claim 30, wherein the realigning comprises identifying the human subject's silhouette.

33. (withdrawn): The method of claim 32, wherein the embedding embeds the watermark information only in the silhouette.

34. (withdrawn): The method of claim 32, wherein the embedding embeds a first watermark component only in the silhouette, and embeds a second watermark component only in an image area that does not correspond to the subject's silhouette.

35. (withdrawn): The method of claim 34, wherein the second component comprises an orientation component.

36. (withdrawn): The method of claim 34, further comprising embedding a third digital watermark component in artwork that is to be associated with the image.

37. (withdrawn): The method of claim 30, wherein the digital camera comprises a video camera.

38. (withdrawn): A method of embedding watermark information in an identification document, comprising:

receiving a digital image of a human subject, the digital image comprising a digital watermark embedded therein, wherein the digital watermark is designed to be removable from the image without significant image degradation, the digital watermark comprising a first set of information that is associated with the human subject;

removing the digital watermark from the digital image to obtain the first set of information;

embedding a second set of information in the digital image; and

printing the digital image on an identification document layer.

39. (withdrawn): The method of claim 38, wherein the second set of information comprises the first set of information.

40. (withdrawn): The method of claim 38, wherein the second set of information corresponds with the first set of information.

41. (withdrawn): The method of claim 38, wherein the first set of information comprises an index, and said method further comprises interrogating a data repository with the index to access the second set of information.

42. (withdrawn): The method of claim 41, wherein the data repository includes auxiliary information, wherein said embedding is controlled at least in part based on the auxiliary information.

43. (withdrawn): The method of claim 38, wherein the first set of information comprises data to authenticate the digital image.

44. (withdrawn): The method of claim 38, wherein the first set of information includes data to indicate a source of the digital image.

45. (withdrawn): The method of claim 44, wherein the source comprises an image capture location.

46. (withdrawn): The method of claim 44, wherein the source comprises a camera identifier.

47. (withdrawn): The method of claim 44, wherein the source comprises a distribution trail.

48. (withdrawn): An identification document comprising:

a substrate;

a first graphic carried by the substrate, the first graphic conveying a photographic image to human viewers thereof,

the first graphic being steganographically encoded to secretly convey first plural bits of

digital data recoverable by computer analysis of said first graphic; and

a laminate layer provided over at least some of the substrate area that includes the first graphic,

wherein the laminate is steganographically encoded to secretly convey second plural bits of digital data recoverable by computer analysis of said laminate, wherein the second plural bits of digital data are steganographically encoded in a manner that differs from the steganographic encoding of the first plural bit of digital data.

49. (withdrawn): The method of claim 48, wherein the steganographically encoded first plural bits of digital data and the steganographically encoded second plural bits of digital data cooperate to verify authenticity of the security document.

50. (withdrawn): The method of claim 48, wherein the computer analysis of the first graphic is performed on data captured through optical scanning of the first graphic, and the computer analysis of the laminate is performed on data corresponding to the surface topology of the laminate.

51. (withdrawn): The method of claim 48, wherein the laminate is encoded through varying the surface texture of the laminate.

52. (previously presented): A programmed computing device storing instructions in memory, said instructions are executable by said programmed computing device to perform the acts of claim 1.

53. (previously presented): A computer readable media comprising instructions stored thereon to cause a multi-purpose electronic processor to perform the acts of claim 1.

54. (previously presented): A programmed computing device storing instructions in memory, said instructions are executable by said programmed computing device to perform the acts of claim 12.

55. (previously presented): A computer readable media comprising instructions stored thereon to cause a multi-purpose electronic processor to perform the acts of claim 12.

56. (previously presented): A programmed computing device storing instructions in memory, said instructions are executable by said programmed computing device to perform the acts of claim 25.

57. (previously presented): A computer readable media comprising instructions stored thereon to cause a multi-purpose electronic processor to perform the acts of claim 25.

EVIDENCE APPENDIX

(No Evidence)

RELATED PROCEEDINGS APPENDIX

(No Related Proceedings)